Saviynt

SOLUTION GUIDE

Saviynt ICAM for DDIL

Disconnected, Denied Intermittent or Limited Bandwidth Environments

The Department of Defense (DOD) has mission requirements to operate in Disconnected, Denied, Intermittent and/or Limited Bandwidth (DDIL) environments. DOD units may be operating in remote or hostile environments, which have low or no bandwidth. When reliable connectivity cannot be achieved, units must retain access to mission-critical systems to conduct assigned missions. A key capability necessary to retain access to mission-critical systems is an Identity, Credentialing and Access Management (ICAM) solution that enables DOD organizations to maintain access to critical systems within a Zero Trust framework.

As part of its Digital Modernization Strategy, the DOD is addressing Command, control, and communications (C3) systems, including capabilities for delivering information services to the tactical edge.

> Ensure the right individuals access the right resources, at the right time, for the right reasons in DDIL environments.
>
> Saviynt

Securing Identity in DDIL Environments

Edge computing systems are limited by size, weight, and power constraints and therefore need clearly defined functionality with disciplined tradeoffs that will provide the required capability. Workloads hosted on edge computing must have the following capabilities:

- Dynamically analyze various sensors
- Adapt their digital signatures
- Selectively transmit relevant information with the appropriate compression algorithms
- Secure access to mission-critical systems in DDIL environments in compliance with the DOD's Zero Trust cybersecurity framework

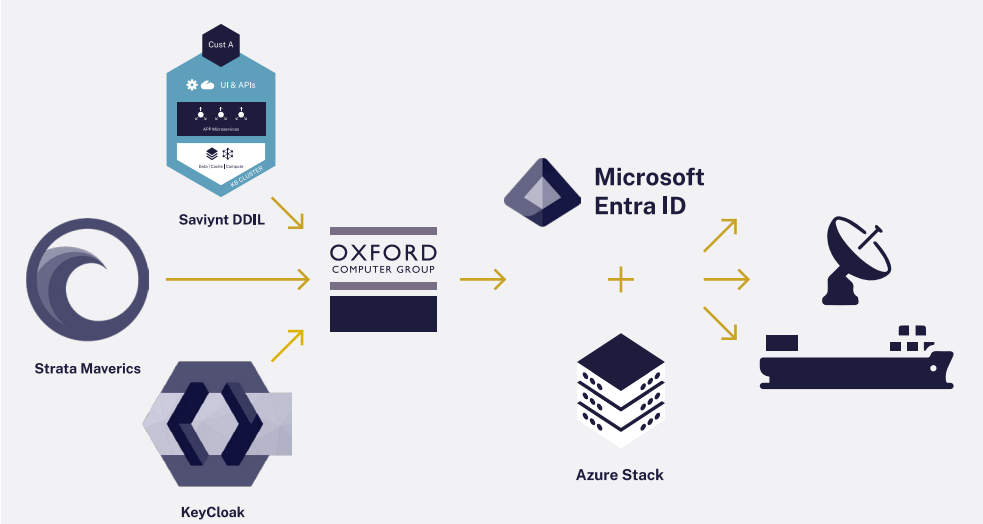
Saviynt is an identity security company that helps governments and commercial organizations modernize identity programs and build Zero Trust foundations.

Saviynt's Identity Cloud is architected for security first, with complete data, network and service isolation. The Identity Cloud is a fully converged platform that unites core identity governance and security capabilities to protect people, data, and infrastructure. Built-in Artificial Intelligence/Machine Learning (AI/ML)-driven analytics enable organizations to contextualize and reduce risk, automate identity lifecycles, and provide smart recommendations to increase security effectiveness. Saviynt uniquely in the market addresses this challenge by providing governance and authorization capabilities to provide a complete solution with other components addressing authentication, authorization, identity data, and governance for full zero trust.

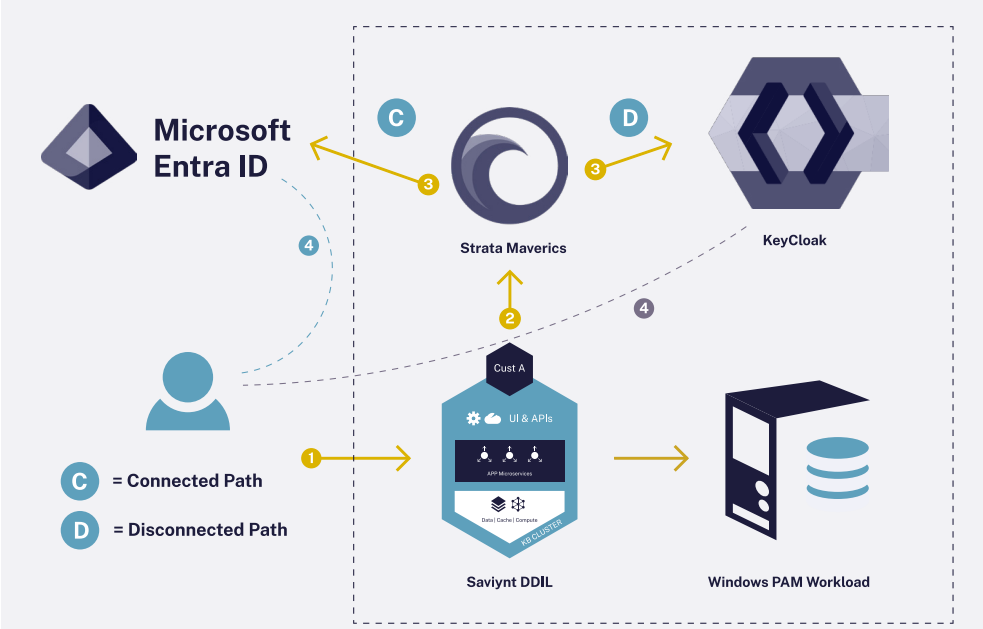
Technical Approach

The solution packages best-of-breed ICAM capabilities that can be quickly deployed and utilized in a variety of tactical and edge environments. Identities from Microsoft Entra ID are provisioned to Saviynt to provide identity services, leveraging Keycloak to provide identity authentication at the edge without the need for large infrastructure build outs.

Solution High Level View



Solution User Experience



Saviynt Identity and Governance & Administration (IGA)

Saviynt's Identity Cloud is a purpose-built, cloud-native identity governance solution that enables the Department of Defense to stay on top of the exploding number of digital identities across on-prem, cloud, and multi-cloud applications environments. Saviynt IGA provides a single pane of glass into a user's access across enterprise data, infrastructure, and applications both in the cloud and on-premises.

Saviynt IGA is a critical aspect of managing access and entitlements in a disconnected (DDIL) state. Key components include:

- **Identity Management:** Allows management and provisioning of user identities and attributes across systems, applications, and networks.
- **Access Management:** Enables controlled access to resources based on user roles, policies, and compliance requirements.
- **Analytics and Reporting:** Offers real-time dashboards, customizable reports, and historical data analysis to gain insights into deployed environments.
- **Auditing and Alerting:** Provides ability to track and record user activity, changes to policies and settings, and access to resources.
- **Connectors:** Saviynt provides connectors for various cloud-based platforms such as Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Services (GCS), as well as traditional enterprise platforms like Active Directory, Exchange, Database support and LDAP. These connectors enable Saviynt to connect and interact with resources within a variety of cloud and on-premises environments.
- **Credential Management:** Allows administrators to securely manage and distribute user credentials across their IT environment.
- **Self-service:** Self-service portals and workflows that enable users to perform certain tasks, such as resetting their own passwords, requesting access to resources, or starting onboarding or offboarding workflows.

ABOUT SAVIYNT

Saviynt empowers enterprises to secure their digital transformation, safeguard critical assets, and meet regulatory compliance. With a vision to provide a secure and compliant future for all enterprises, Saviynt's cutting-edge solutions have been recognized as industry leaders. For more information, please visit www.saviynt.com.

Saviynt

Headquarters, 1301 E
El Segundo Bl, Suite D, El Segundo, CA
90245, United States

310. 641. 1664 | info@saviynt.com
www.saviynt.com